FortiOS 6.2 – Whats New

FortiManager 6.2

Martin Ruesch – Security Consultant ALSO Schweiz

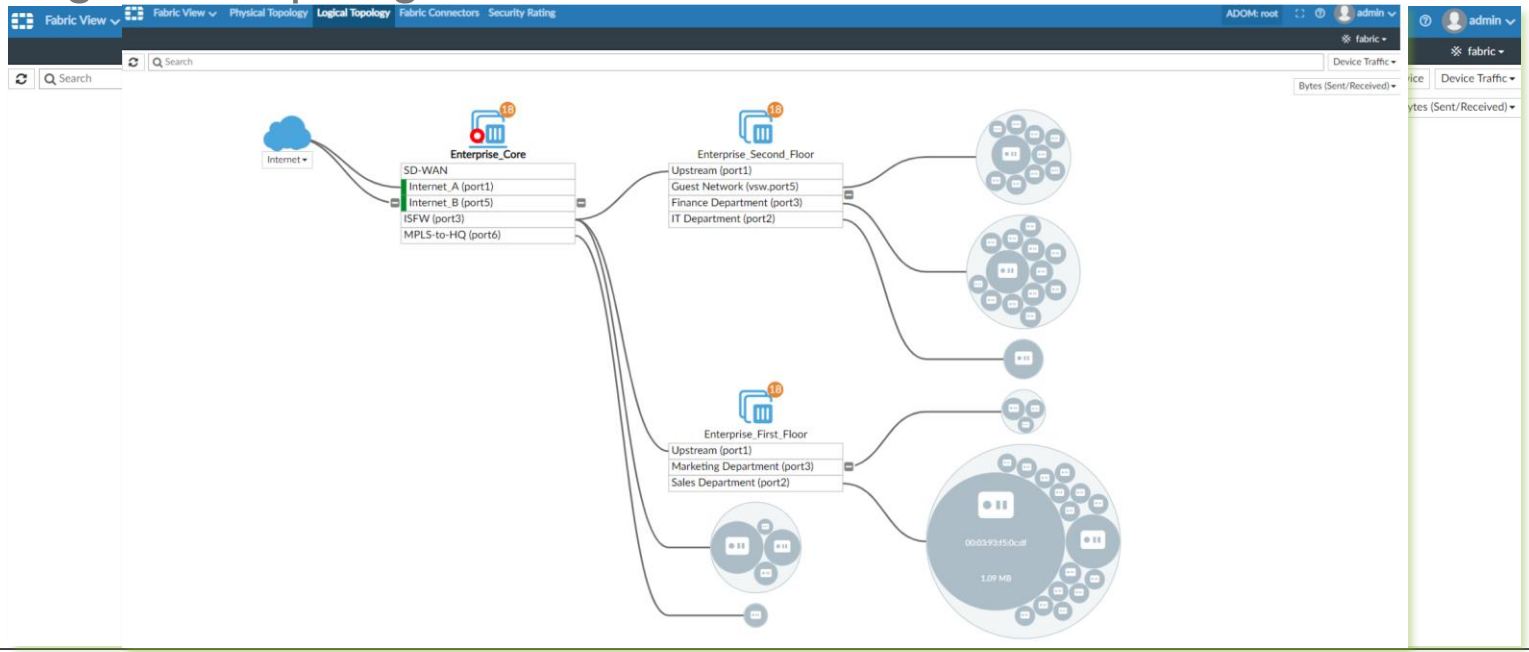
Agenda

- Expanding Fabric
- SD-WAN
- Multi-Cloud
- Usability
- Compliance
- Other

Expanding Fabric

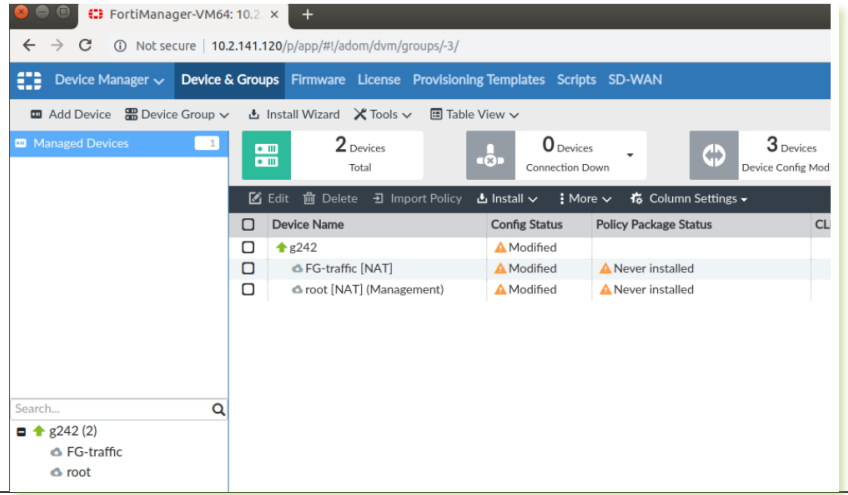
Security Fabric Deployments – Physische Topologie

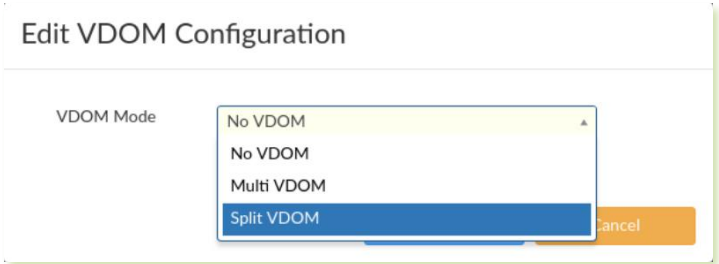
- Physische Topologie
- Logische Topologie



Split Task VDOM Mode Support

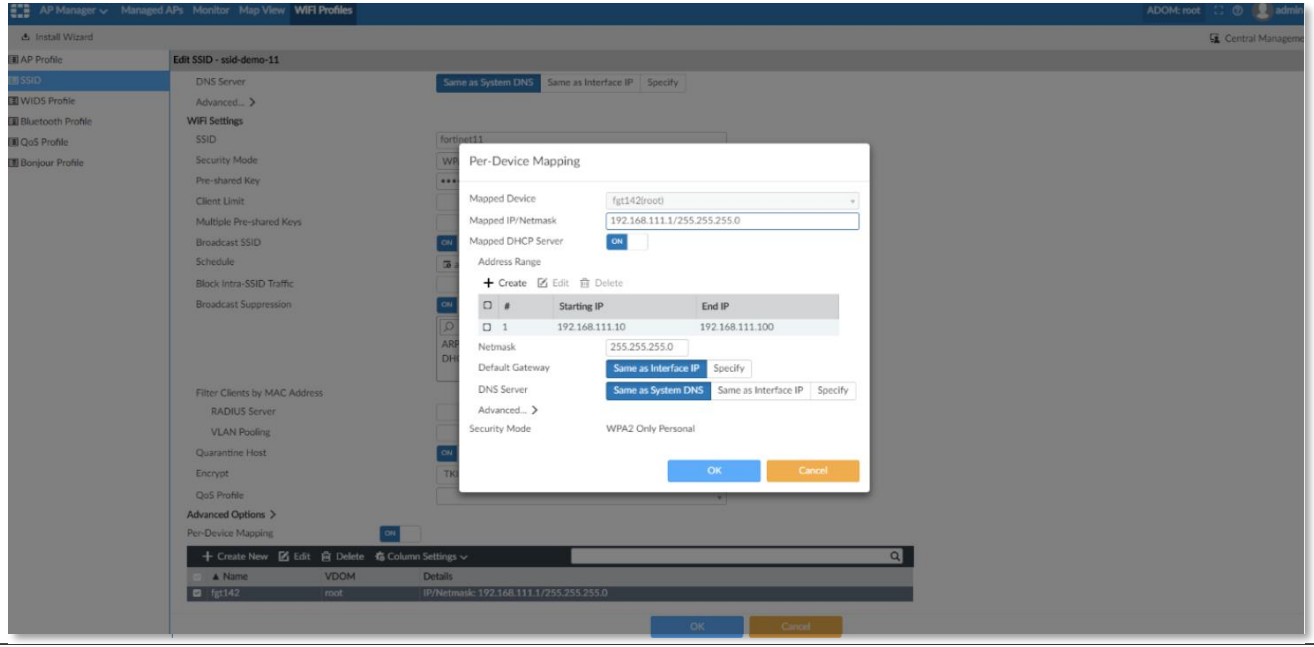
- *No VDOM* es können keine VDOMs erstellt werden.
- *Multi VDOM* so viele VDOM wie die Lizenz hergibt können erstellt werden
- *Split VDOM* speziell mit 2 VDOM (1 Regulär, 1 Management)





Dynamic Mapping für SSID

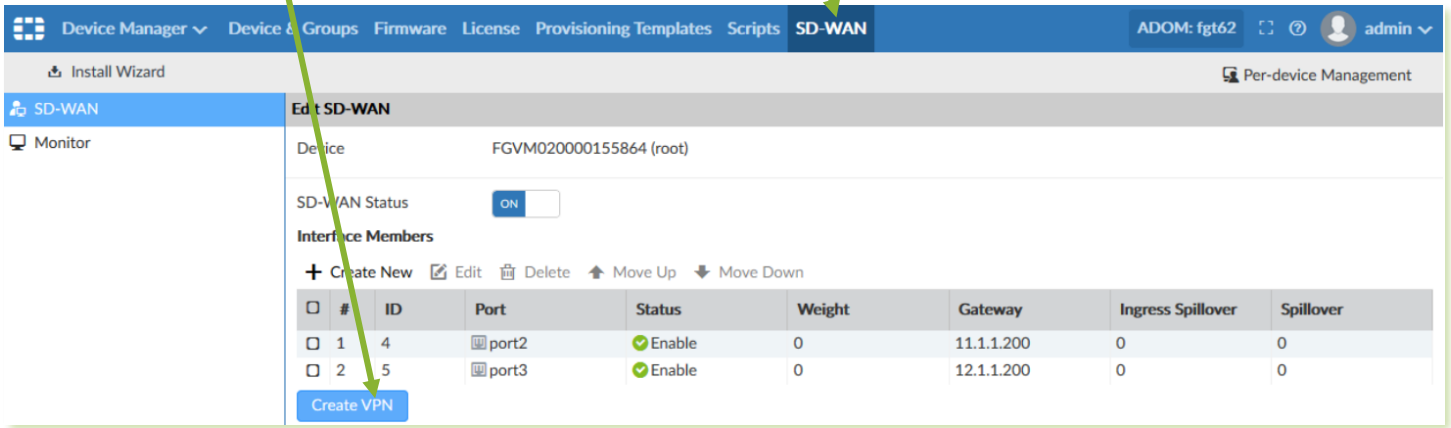
- Dynamisch Netze einer SSID per FortiGate zuweisen (gleiche SSID verschiedene Netze)



SD-WAN

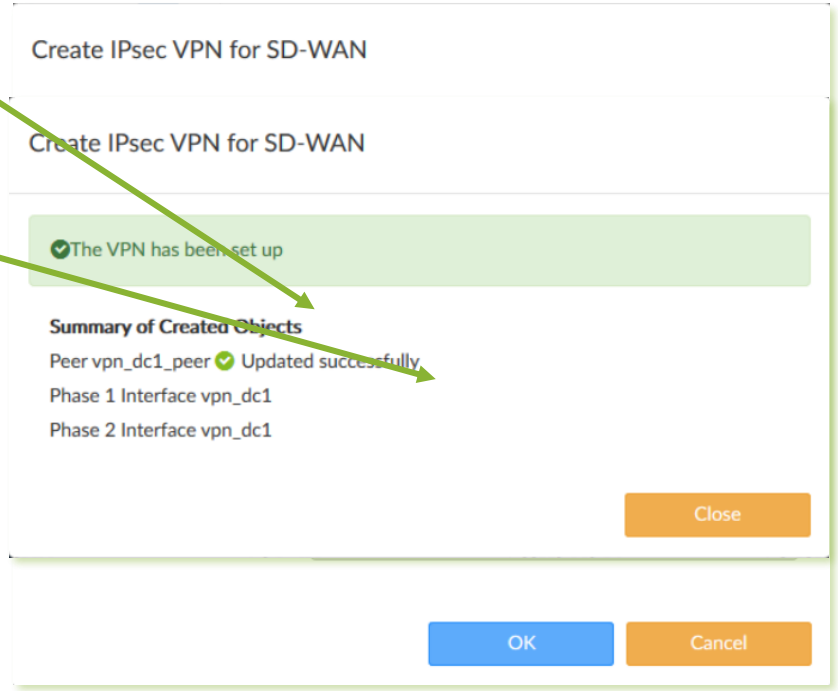
IPSEC Wizard in Device Manager

- System Settings →All ADOMS editieren der ADOM. Deaktivieren der SD-WAN Option im Central Management
- Device Manager → SD-WAN jetzt Device oder ADOM auswählen.
- Jetzt Create VPN unter den Interface Members auswählen.



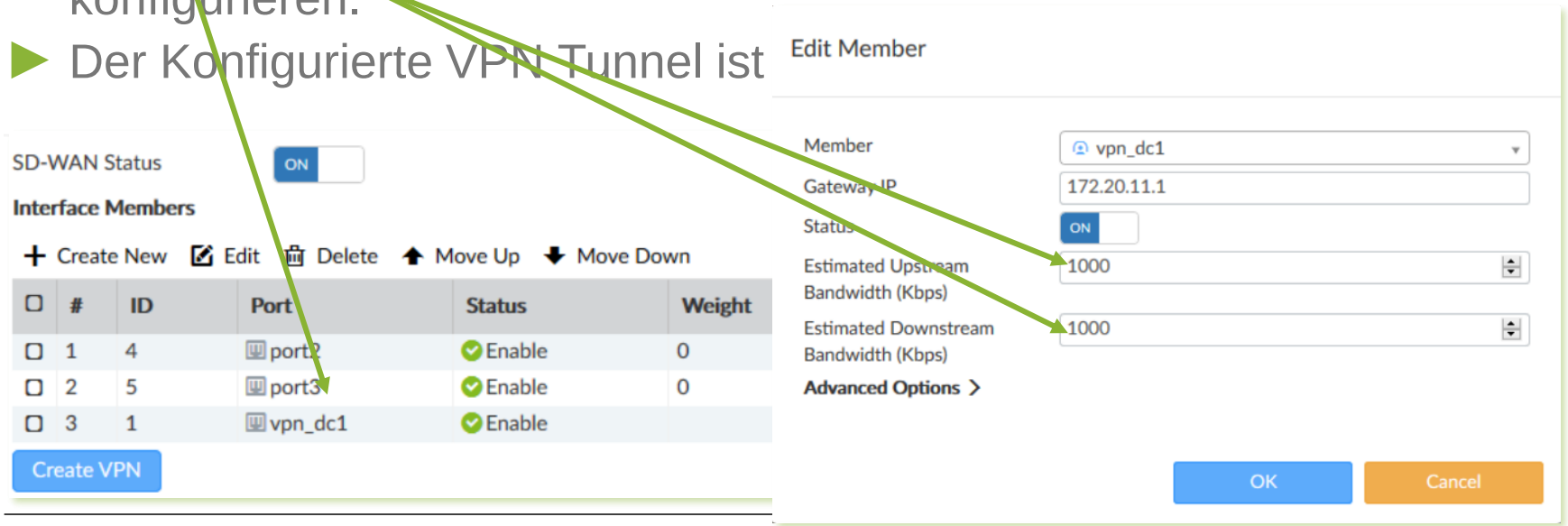
IPSEC Wizard in Device Manager

- Die ausgehenden Interfaces konfigurieren
- Authentication Methode: Pre-shared Key oder Zertifikat auswählen.
- Mit OK bestätigen, dann wird der Tunnel automatisch generiert.



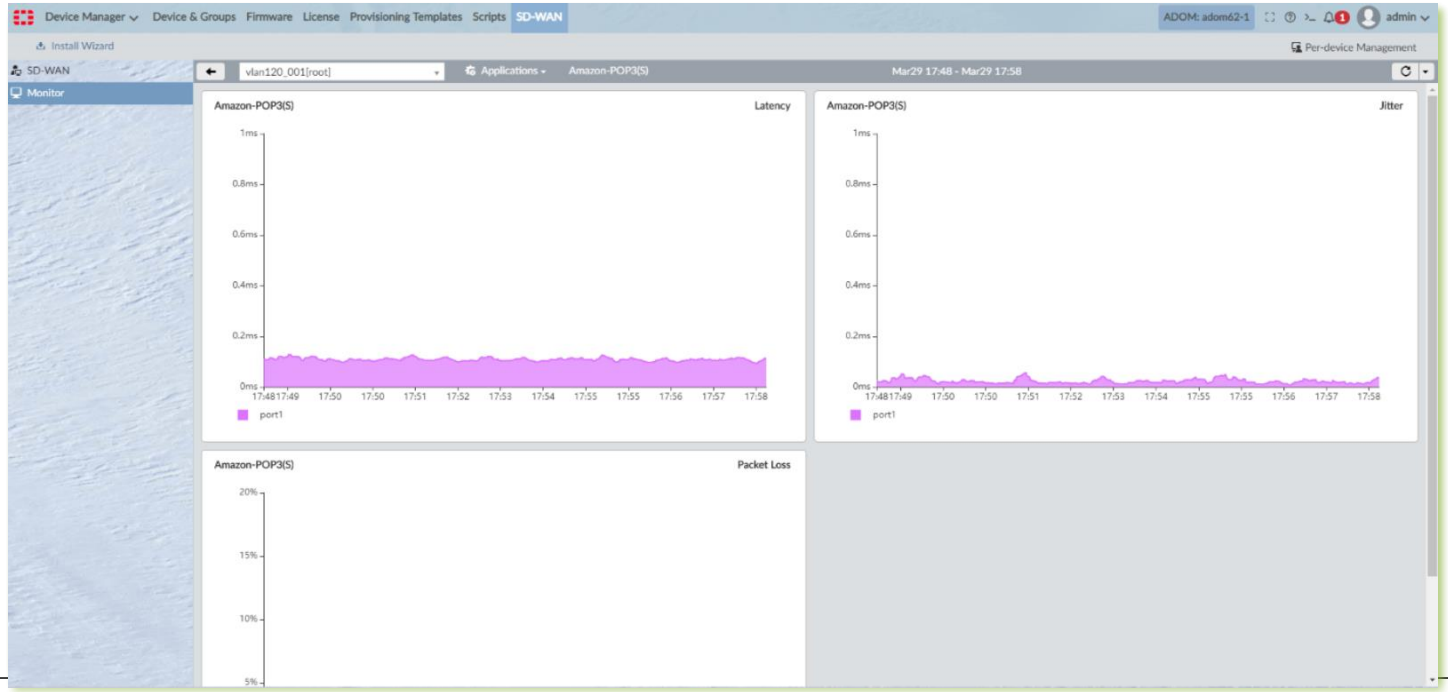
IPSEC Wizard in Device Manager

- Das automatisch erstellte VPN-Interface wird in der SD-WAN Interface Member Liste jetzt aufgeführt.
- Dem VPN Interface die Gateway IP und Up/Downstream konfigurieren.
- Der Konfigurierte VPN Tunnel ist



SD-WAN History Monitoring

- Device/Interface Bandwidth, Application Bandwidth, Latency, Jitter, Packet Loss History



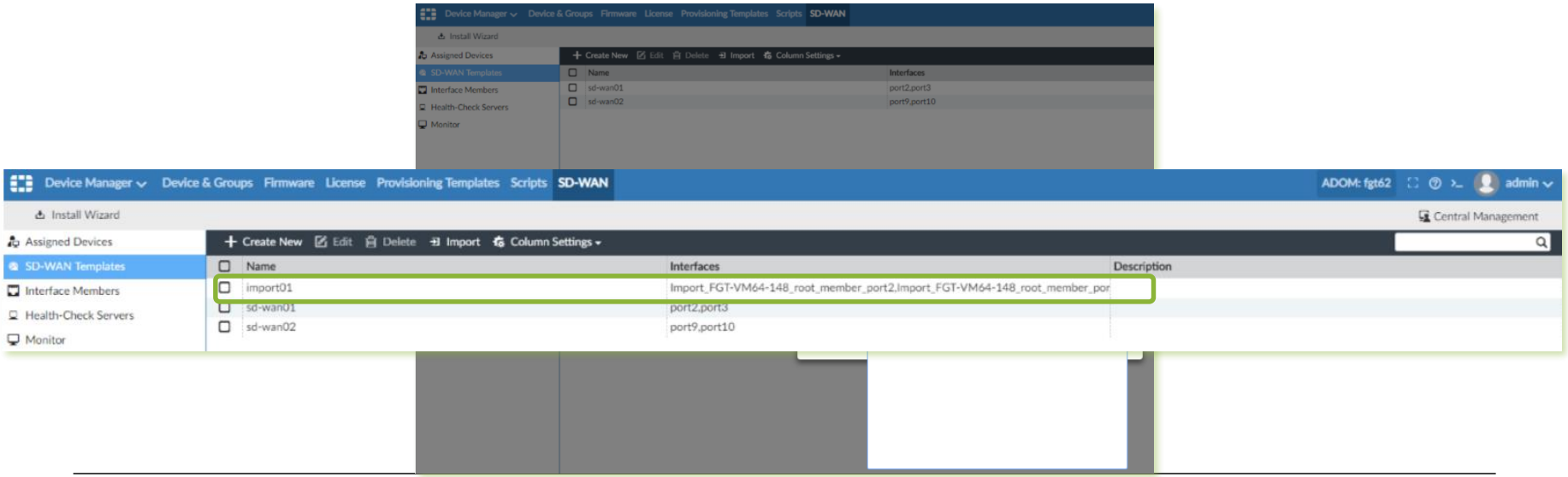
SD-WAN History Monitoring

- Die Funktion muss auf der CLI aktiviert werden.
- Default mässig ist die Funktion disabled
- Wenn die Funktion disabled ist, werden nur die letzen zehn Minuten angezeigt.

```
config system admin setting
       set sdwan-monitor-history [enable|disable]
end
```

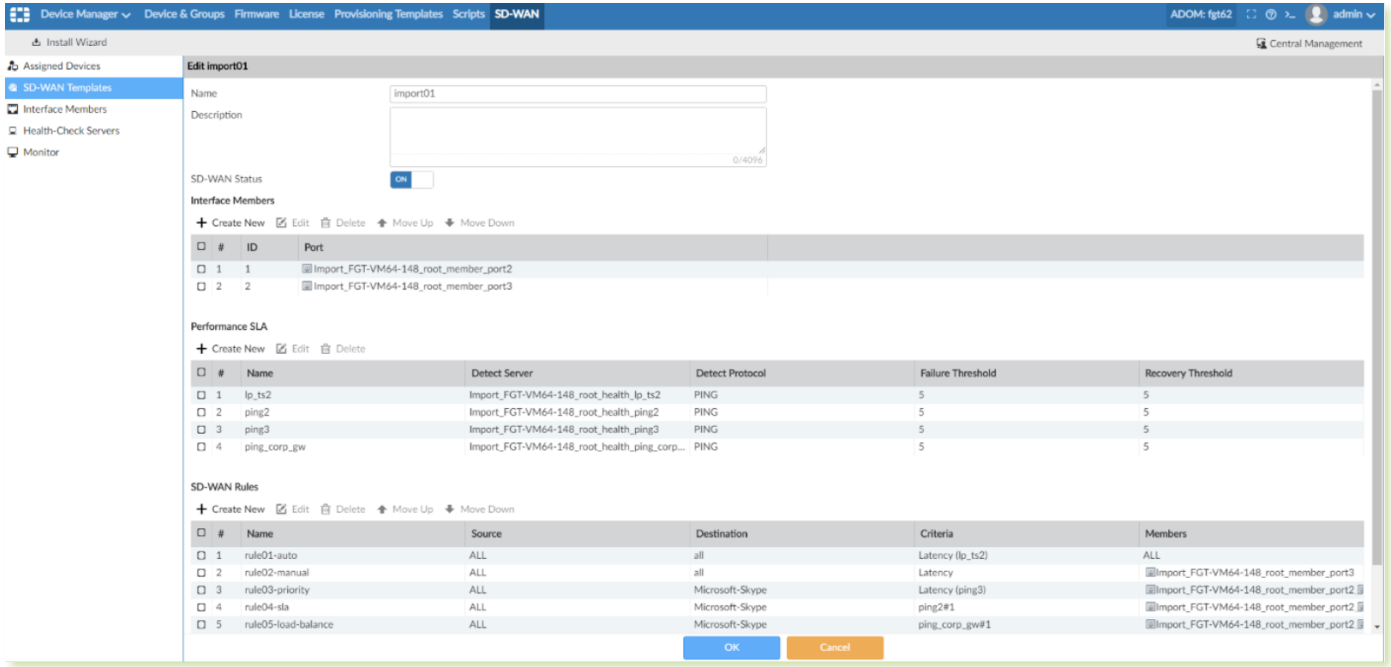
SD-WAN Templates vom Device importieren

- Device Manager → SD-WAN → SD-WAN Templates
- Nach dem import wird das Template angezeigt.



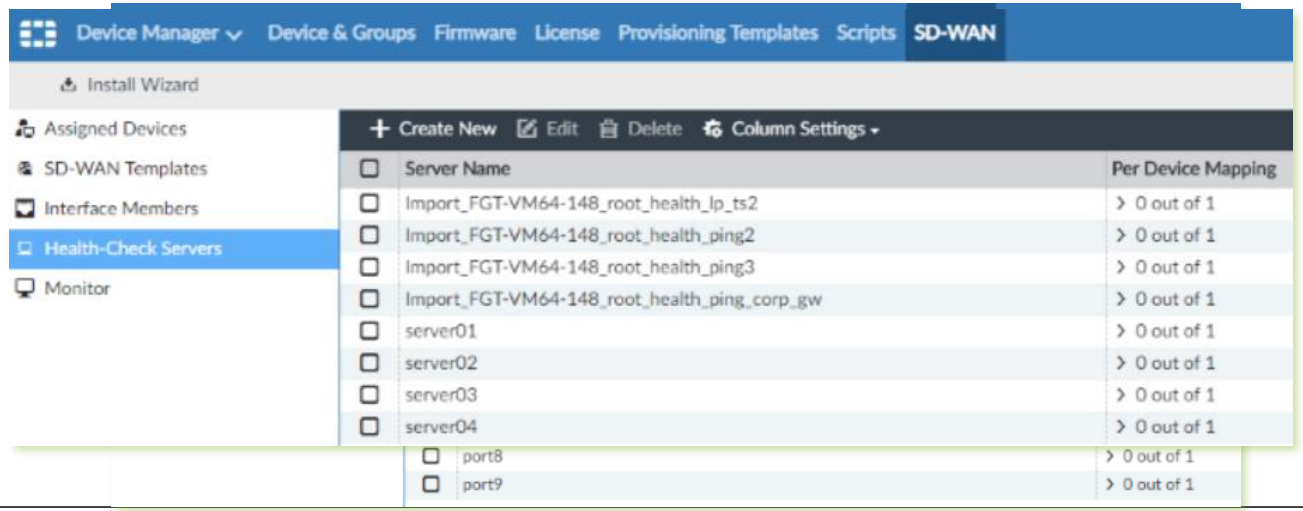
SD-WAN Templates vom Device importieren

- Die Interface Members, Performance SLA und SD-WAN-Regeln werden ebenfalls importiert.



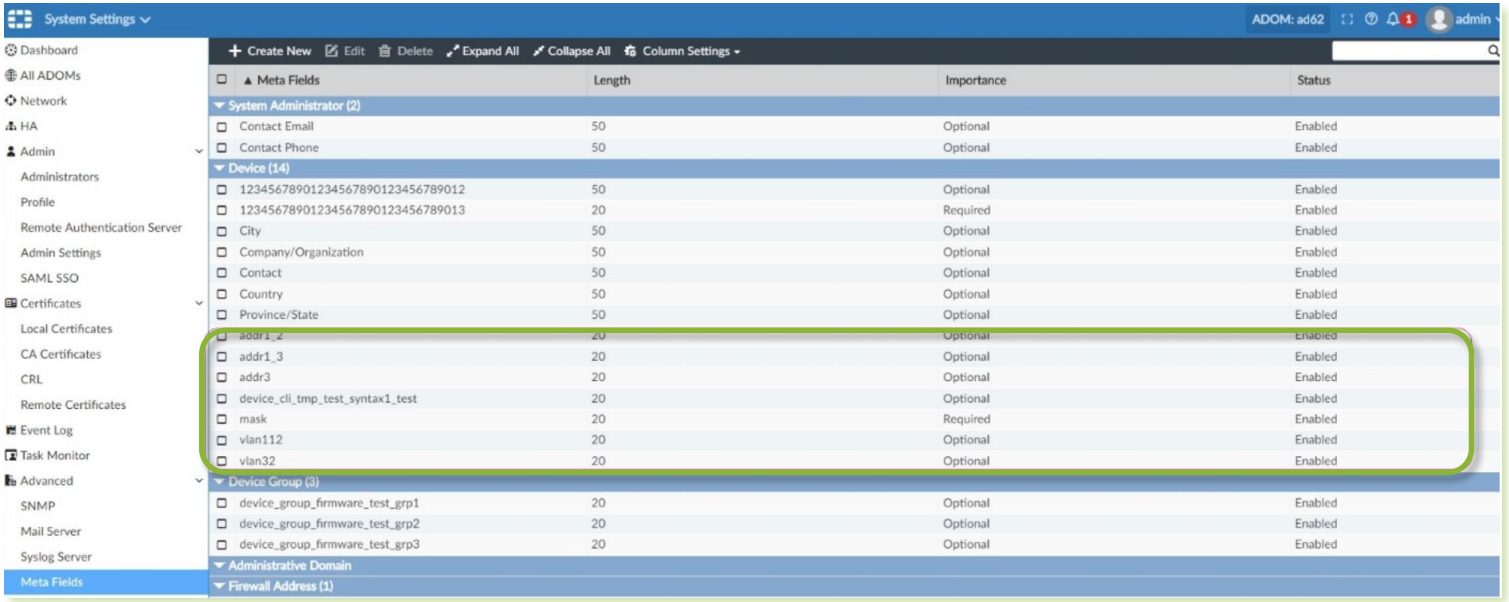
SD-WAN Templates vom Device importieren

- Nach dem import wird ein Name für jedes Mitglied generiert: Import_{device-name}_vdom-name}_member_{interface-name}
- Dasselbe wird auch mit den Healthcheck Server generiert: Import_{device-name}_{vdom-name}_health_{health-check-name}



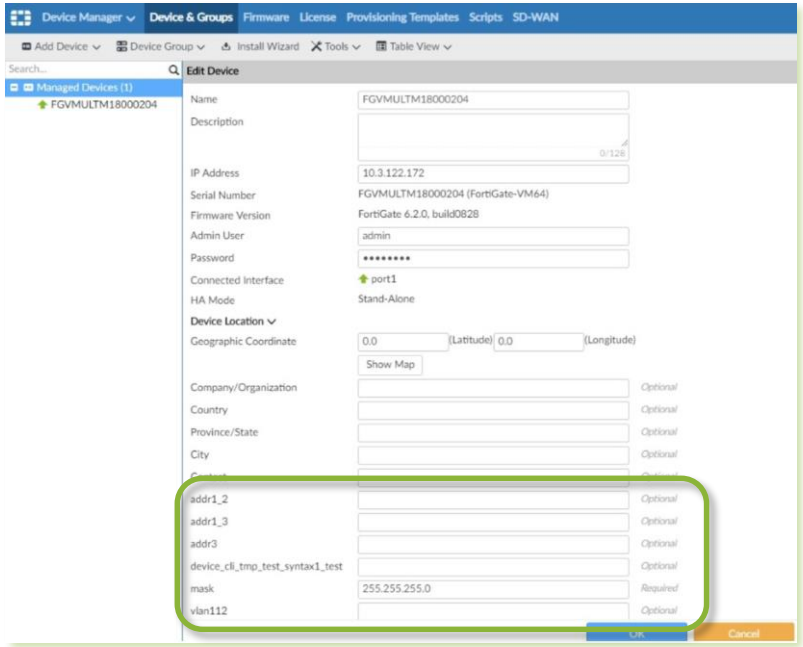
Zero Touch Provisioning - CLI Template mit Variablen

- Bei den Meta Felder (Meta Fields) werden die Variablen definiert, welche für die CLI Vorlage verwendet werden.



Zero Touch Provisioning - CLI Template mit Variablen

- Im Device Manger beim entsprechenden Device die gewünschten Werte den Variablen zuweisen.

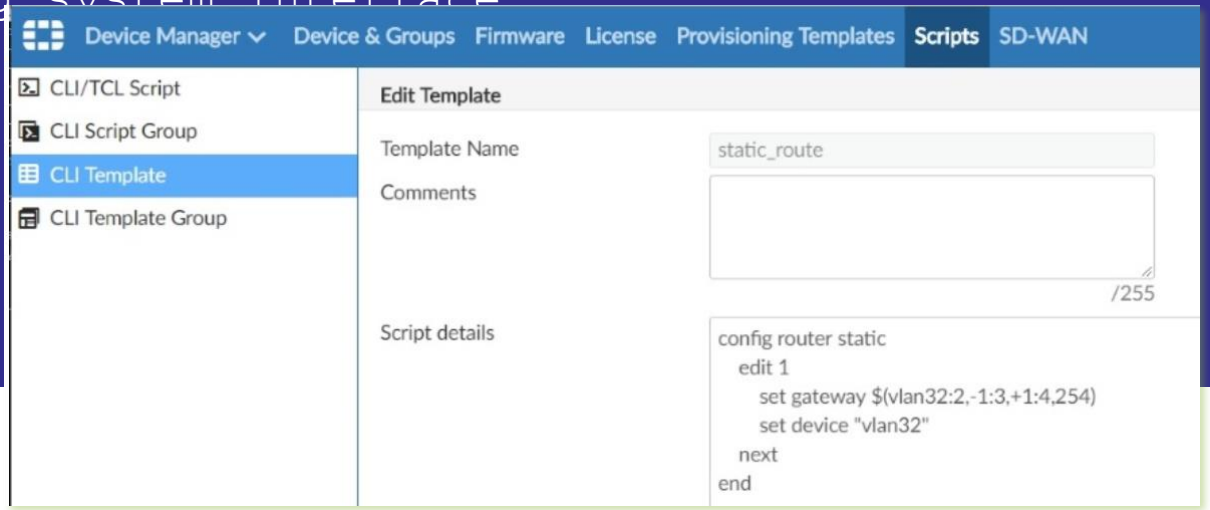


Zero Touch Provisioning - CLI Template mit Variabeln

- Beispiele eines CLI Templates:

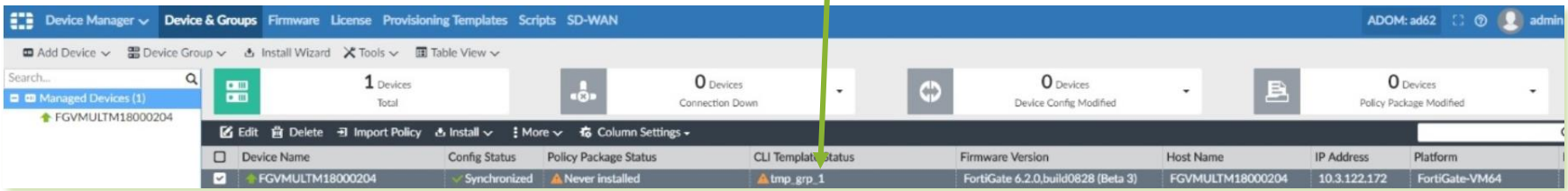
```
config system interface


end
```



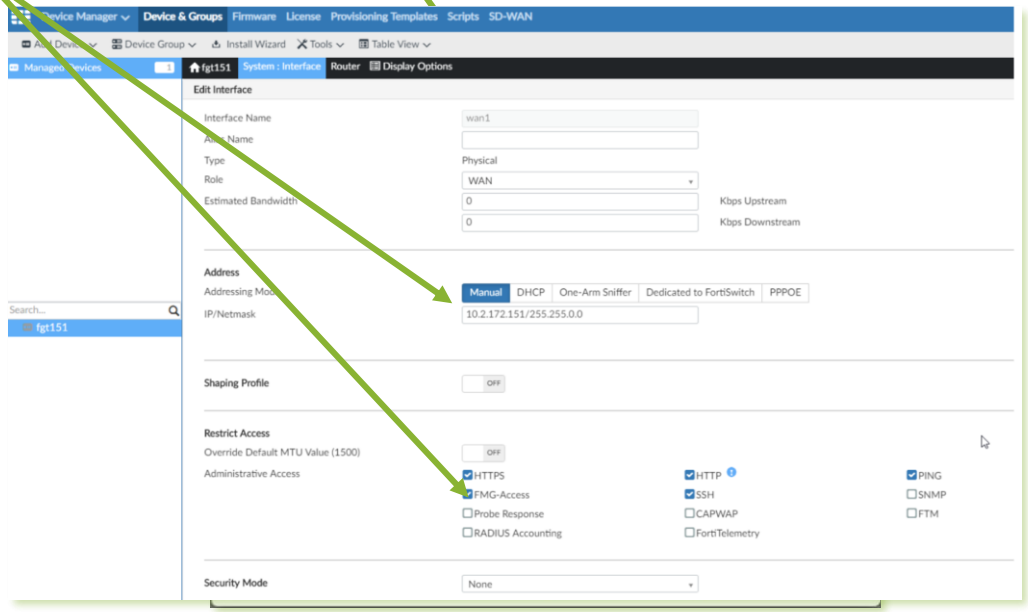
Zero Touch Provisioning - CLI Template mit Variablen

- Im Geräte Manager kann man die zugewiesenen Templates sehen



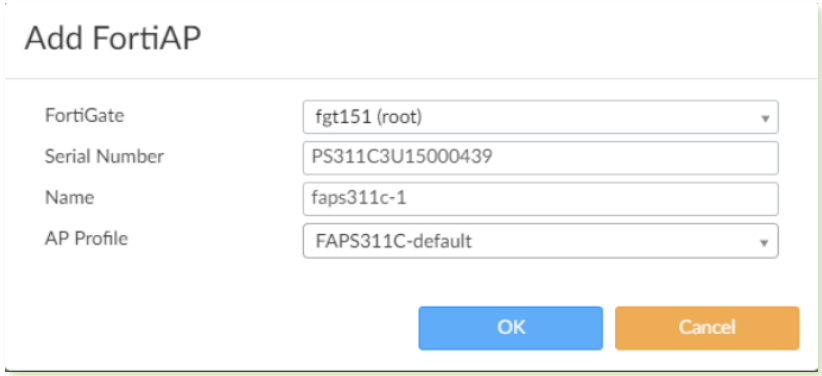
Zero Touch Provisioning für FortiAP

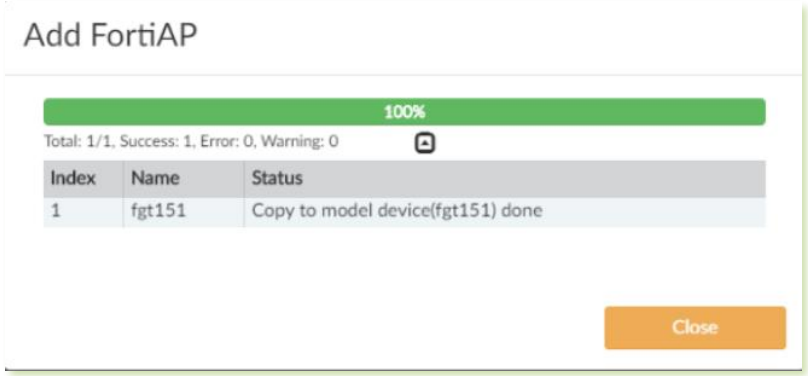
- FortiGate mit Seriennummer im FMG erfassen
- Interface Parameter für den Zugriff des FMG konfigurieren

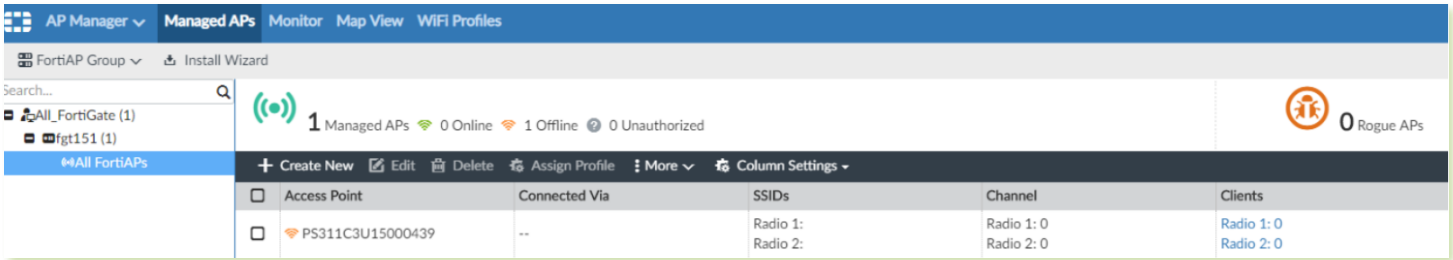


Zero Touch Provisioning für FortiAP

- Im AP Manager den AP mit seiner Seriennummer hinzufügen

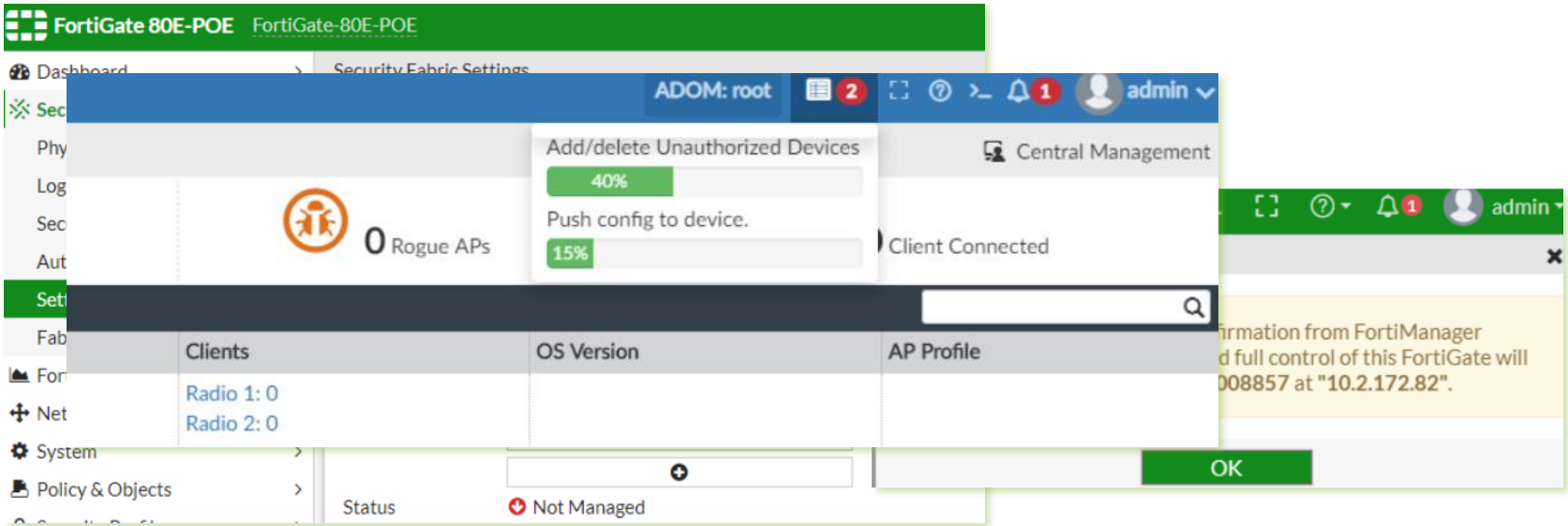






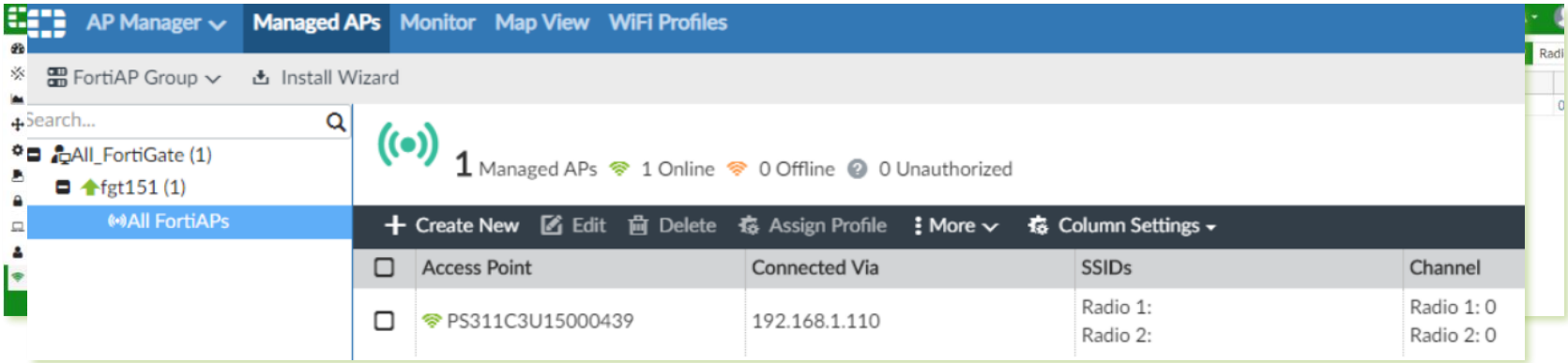
Zero Touch Provisioning für FortiAP

- AP und FMG Netzwerktechnisch miteinander verbinden
- Auf der FortiGate den FortiManager konfigurieren.
- Auf dem FortiManager den Status der Auto-Link Funktion überprüfen



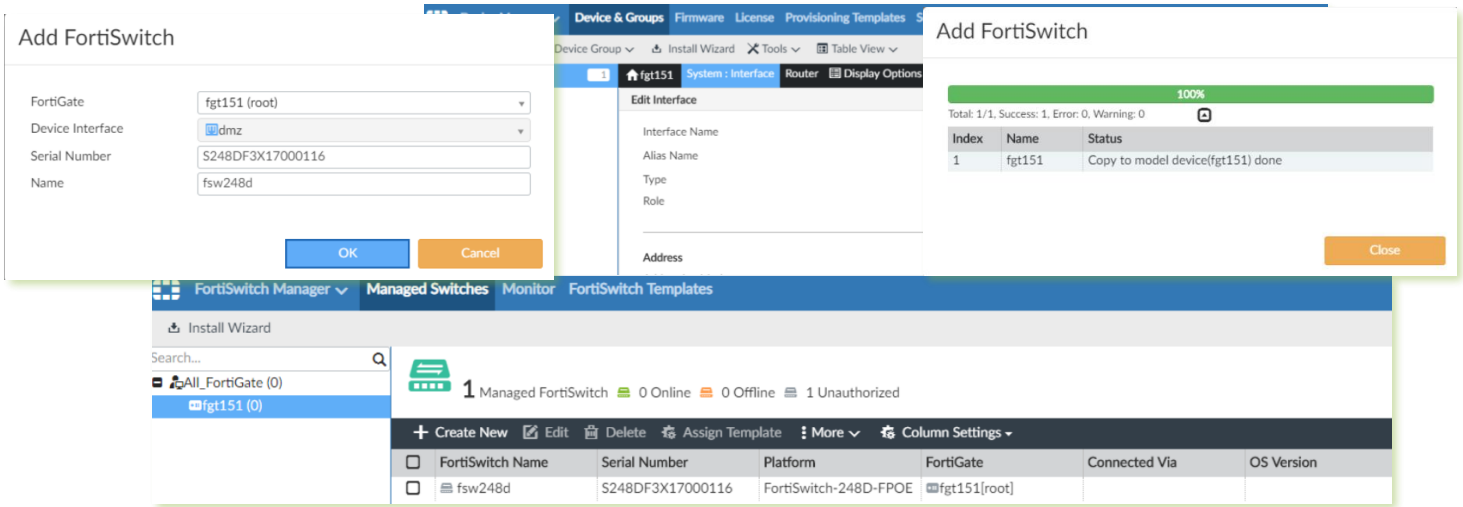
Zero Touch Provisioning für FortiAP

- Auf der FortiGate den Accesspoint überprüfen ob er aktiviert wurde
- Im FortiManager sollte man den AP jetzt auch online sehen



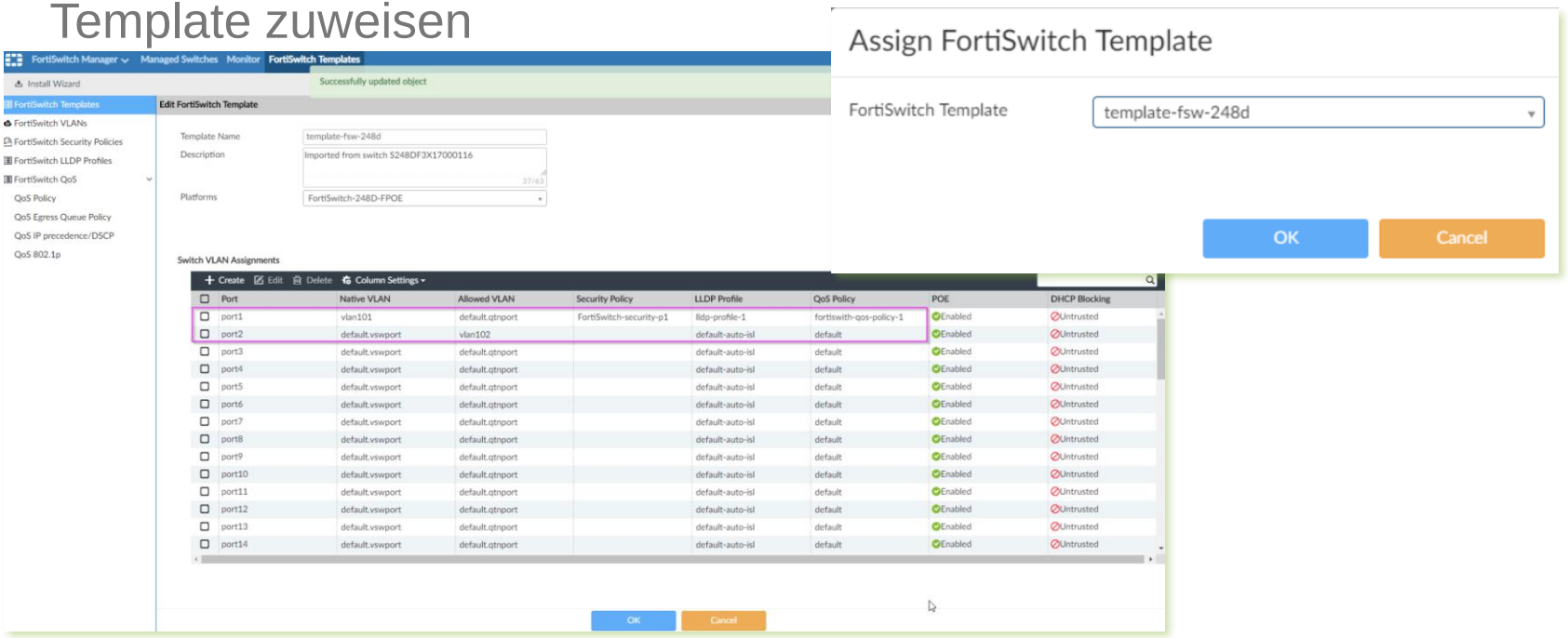
Zero Touch Provisioning für FortiSwitch

- FortiGate auf dem Manager einbinden und Interface für management konfigurieren.
- FortiLink auf Interface konfigurieren und IP Adresse definieren
- FortiSwitch mit Serienummer hinzufügen



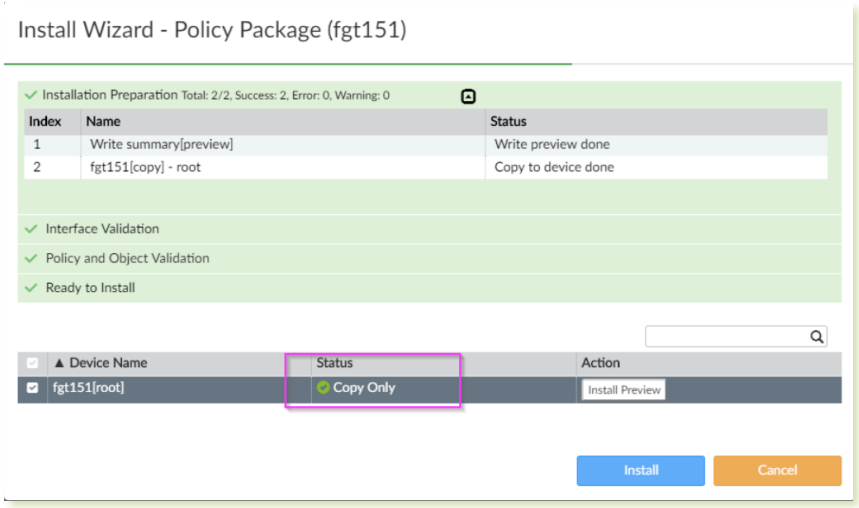
Zero Touch Provisioning für FortiSwitch

- Ein FortiSwitch Template auf dem FortiManager erstellen und das Template zuweisen



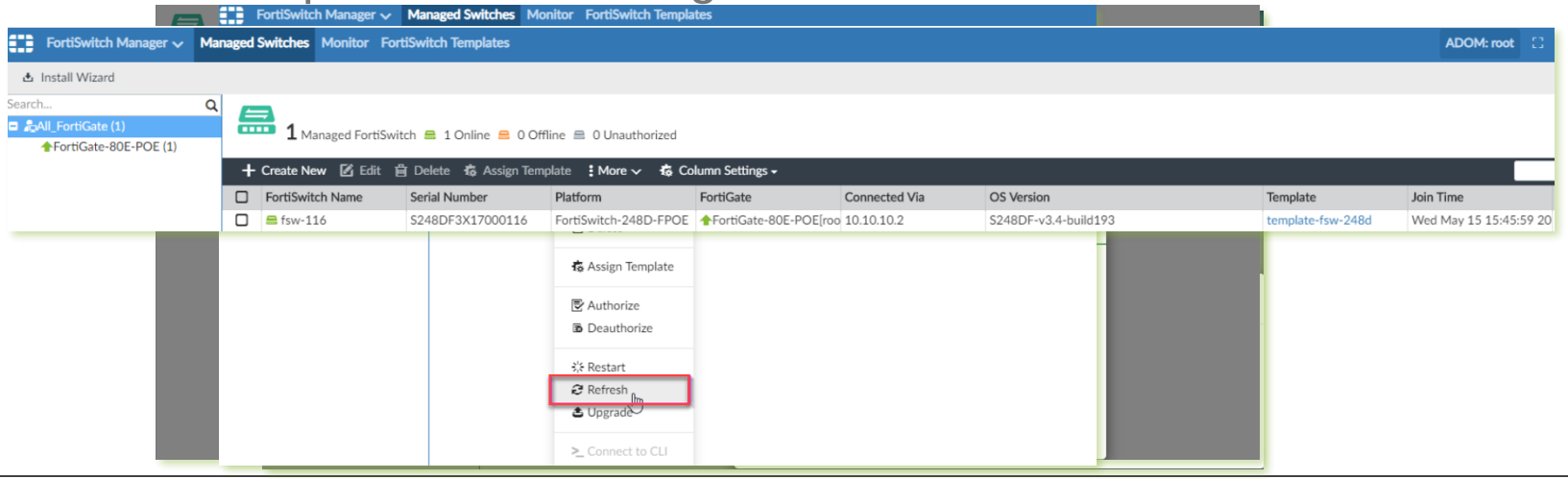
Zero Touch Provisioning für FortiSwitch

- Policy Packet für das Model Device erstellen und dies auf das FortiGate Model kopieren.



Zero Touch Provisioning für FortiSwitch

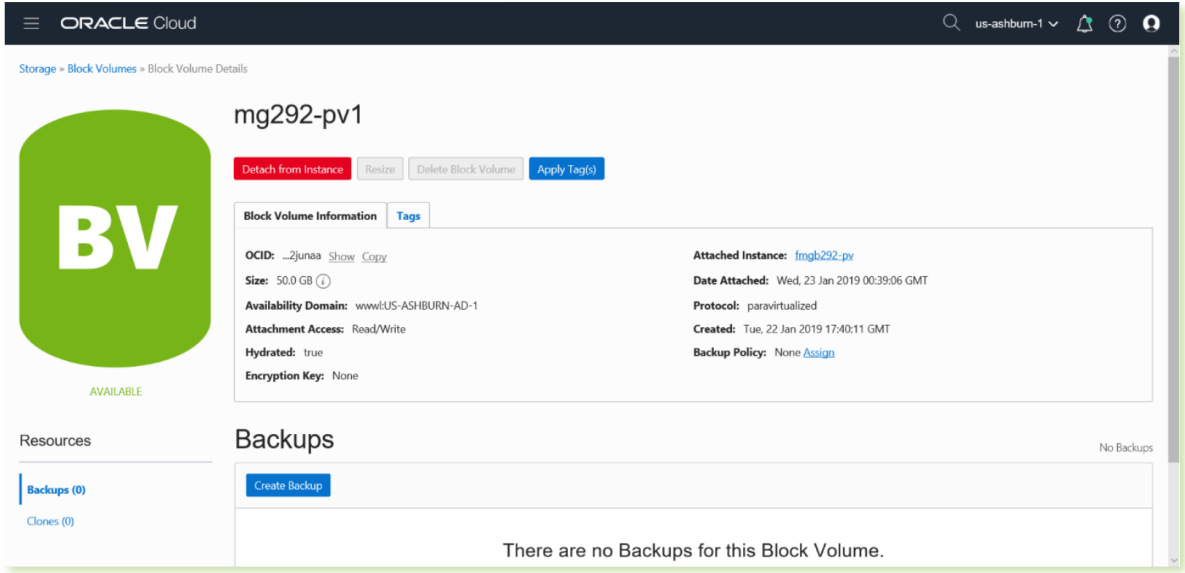
- FortiGate im Manager einbinden
- Template zuweisen
- Konfiguration auf die FortiGate deployen
- Nach dem pushen der Konfiguration, im FMG den Status refreshen



Multi-Cloud

Oracle Cloud - Paravirtualized Mode Support

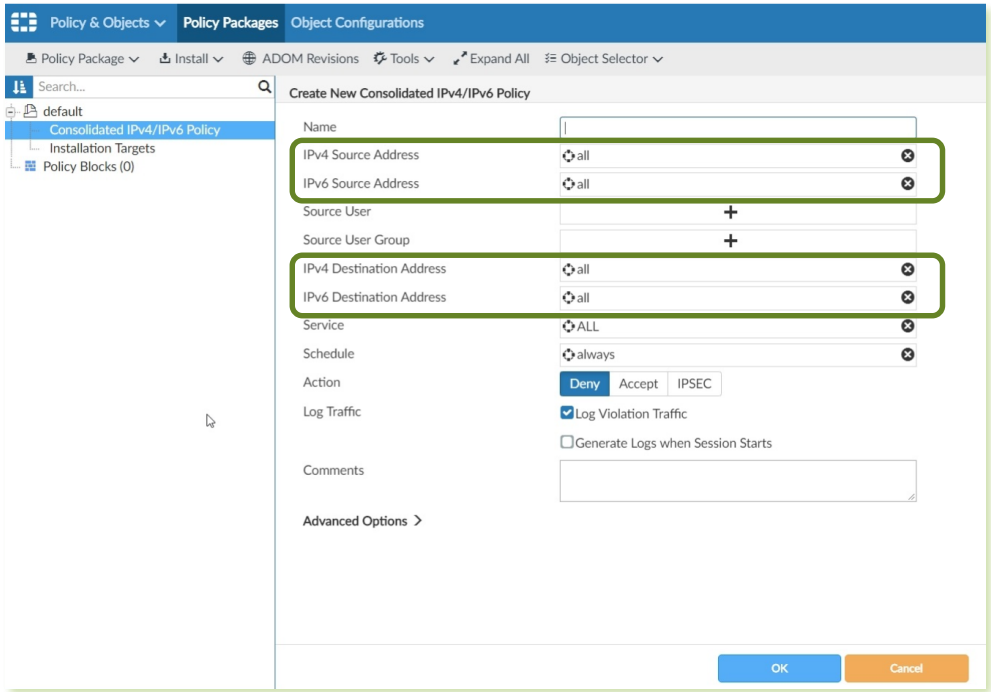
- Der FortiManager unterstützt ab 6.2 den paravirtualisierten Modus in der Oracle Cloud.



Usability

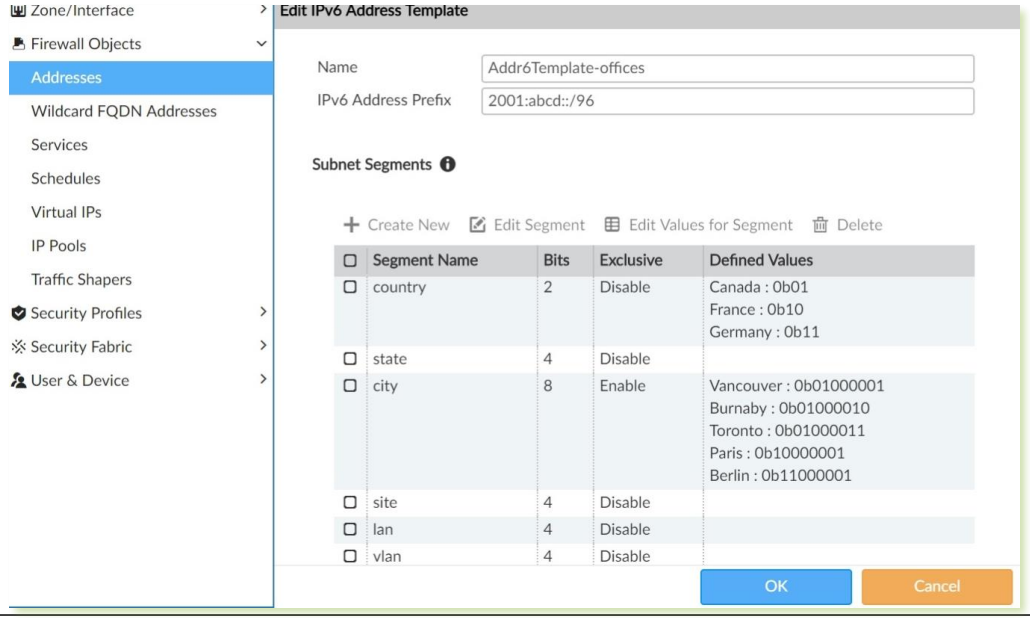
Konsolidierter Firewall-Modus

- IPv4 und IPv6 Regeln in einem erstellen



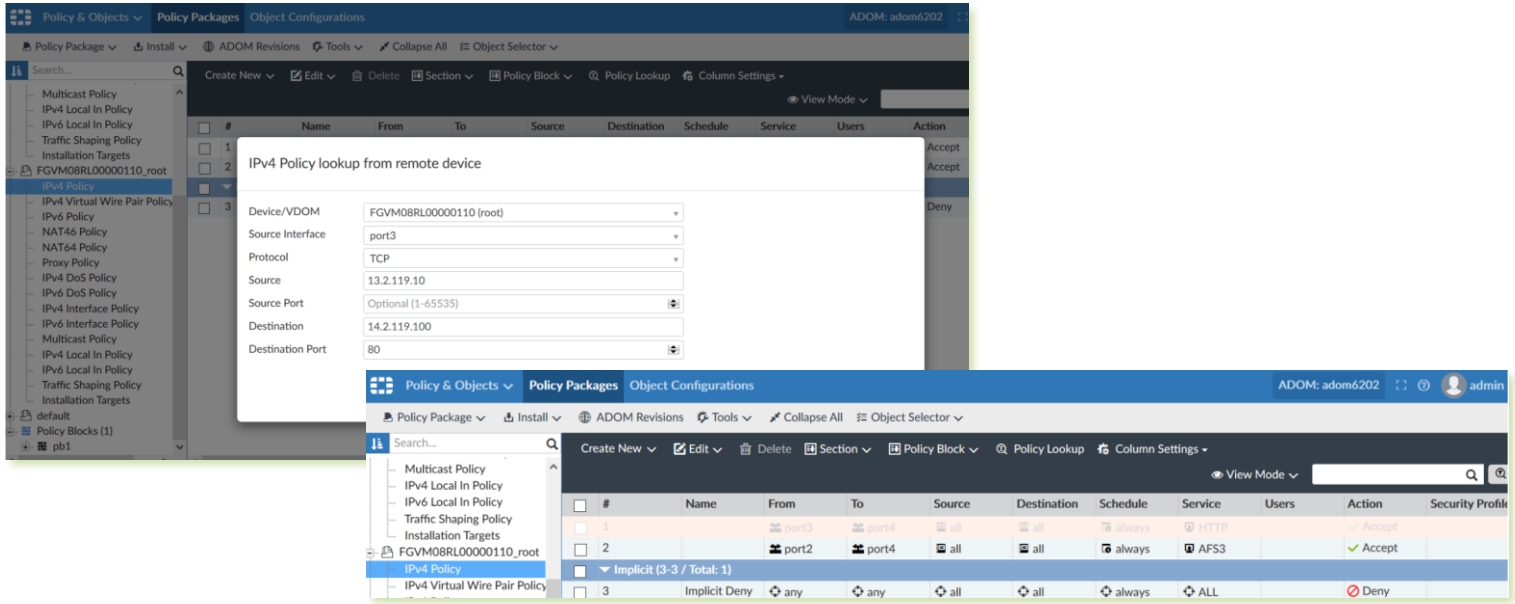
IPv6 Templates

- Das IPv6-Template ermöglicht es Administratoren, eine IPv6-Vorlage mit vordefinierten Parametern zu erstellen



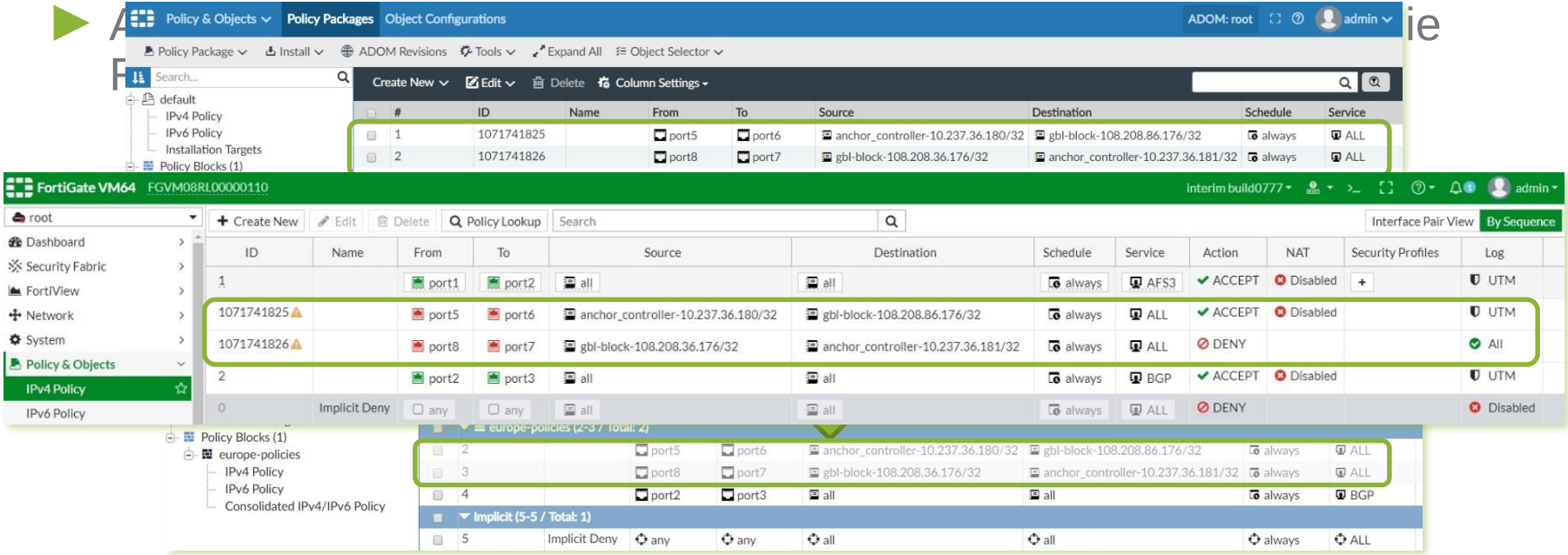
Policy und Routen Lookup

- Policy und Routen können anhand von Eingaben gesucht werden.
- Die Funktionen zur Policy- und Routensuche werden beide über die FortiGate-API aufgerufen, da diese den Echtzeitzustand der FortiGate benötigen.



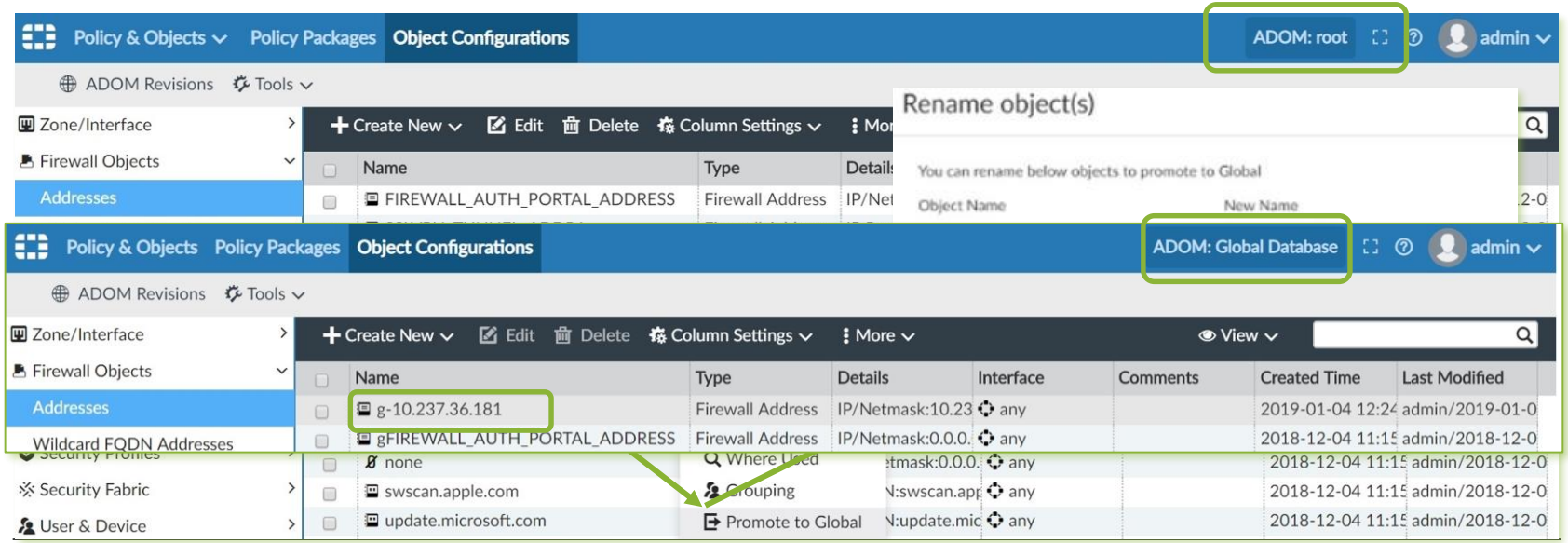
Policy Blocks

- Regeln können in Blöcke definiert werden
- Die Blöcke können im Regulären Policy Pack hinzugefügt werden.
- A… ie F…



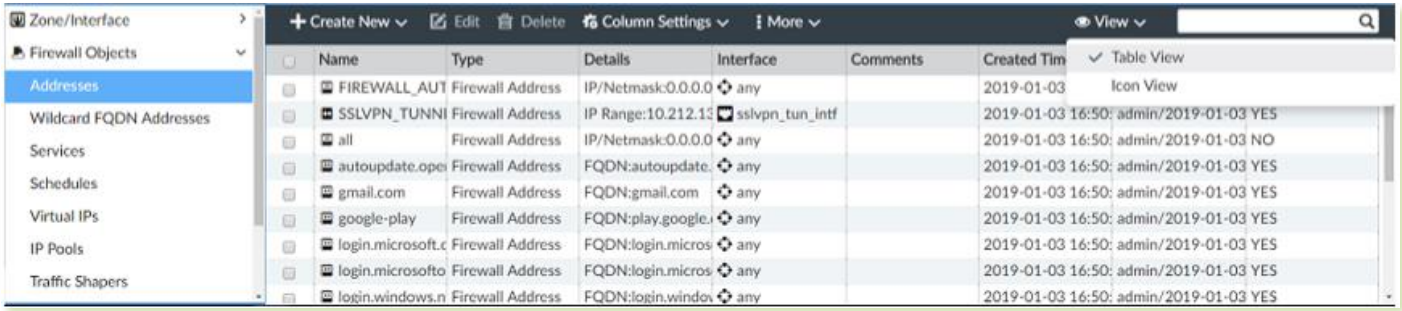
Promote Objects LOCAL → GLOBAL

- Objekte können von einer ADOM in die Globale Datenbank verschoben werden
- Globale Objekte können für alle ADOMs benutz werden



Adresssymbol / Kachelansicht

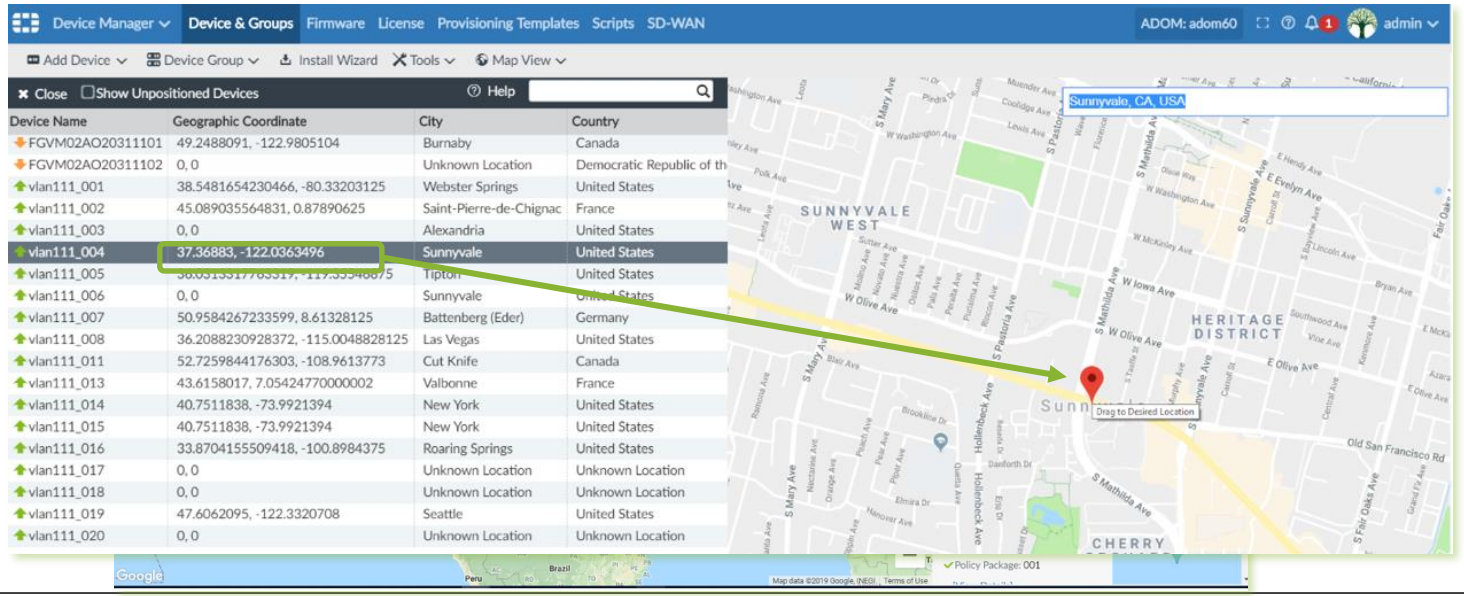
- Adresssymbol Ansicht:



- Kachel Ansicht

Device Manager Map View

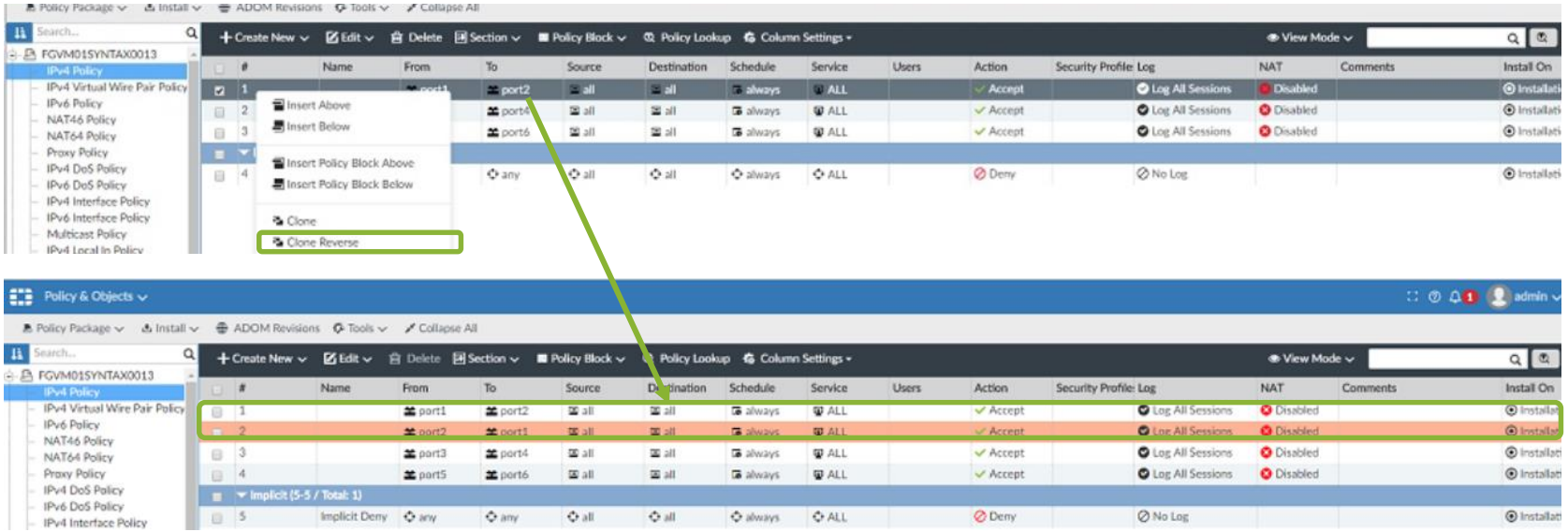
- Grün = Device I.O
- Detail-Karte, Koordinaten der FortiGate angeben
- Gelb = Warnung → Synchronisation nicht I.O FortiGate und FMG
- Rot = Fehler → Installation Fehlgeschlagen, Gerät nicht erreichbar.



Device Name	Geographic Coordinate	City	Country
FGVM02AO20311101	49.2488091, -122.9805104	Burnaby	Canada
FGVM02AO20311102	0, 0	Unknown Location	Democratic Republic of th
vlan111_001	38.5481654230466, -80.33203125	Webster Springs	United States
vlan111_002	45.089035564831, 0.87890625	Saint-Pierre-de-Chignac	France
vlan111_003	0, 0	Alexandria	United States
vlan111_004	37.36883, -122.0363496	Sunnyvale	United States
vlan111_005	[illegible]	Tipton	United States
vlan111_006	0, 0	Sunnyvale	United States
vlan111_007	50.9584267233599, 8.61328125	Battenberg (Eder)	Germany
vlan111_008	36.2088230928372, -115.0048828125	Las Vegas	United States
vlan111_011	52.7259844176303, -108.9613773	Cut Knife	Canada
vlan111_013	43.6158017, 7.05424770000002	Valbonne	France
vlan111_014	40.7511838, -73.9921394	New York	United States
vlan111_015	40.7511838, -73.9921394	New York	United States
vlan111_016	33.8704155509418, -100.8984375	Roaring Springs	United States
vlan111_017	0, 0	Unknown Location	Unknown Location
vlan111_018	0, 0	Unknown Location	Unknown Location
vlan111_019	47.6062095, -122.3320708	Seattle	United States
vlan111_020	0, 0	Unknown Location	Unknown Location

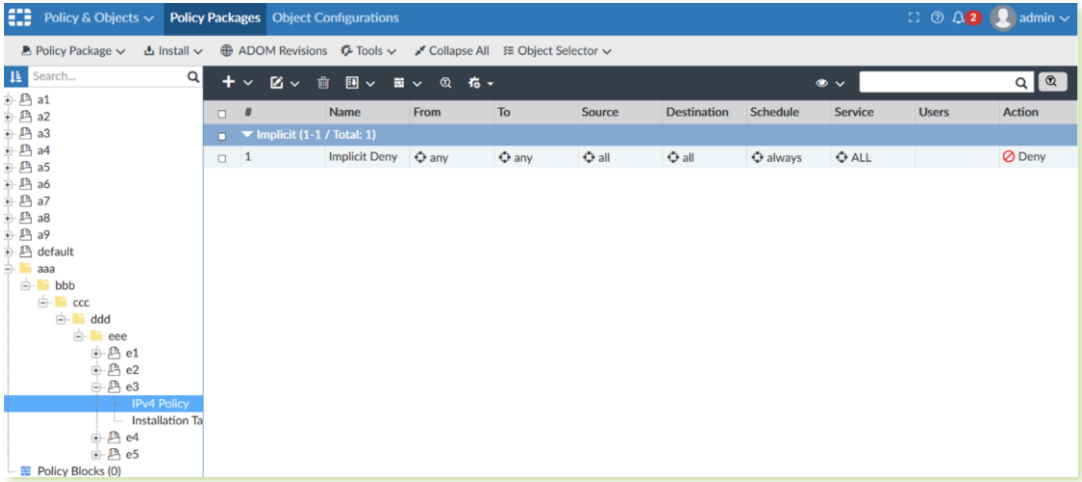
Klonen von Reversen Policies

- Policy gegengleich konfigurieren (Source und Destination umdrehen)



Admin Preference - Policy Package Cookie

- Zuletzt geöffnetes Policy Package wird beim erneuten einloggen geöffnet.
- Das zuletzt bearbeitete Objekt wird beim erneuten einloggen wieder geöffnet

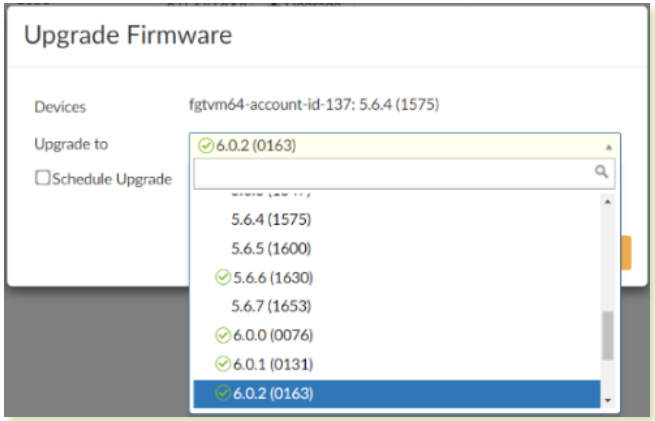


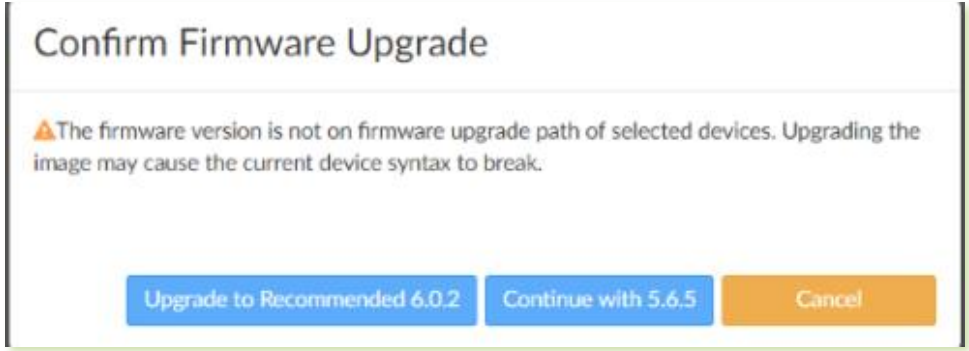
Upgraden von Devices

- Warnung beim Upgrade auf eine höhere Version von FortiOS als FortiManage

Upgraden von Devices

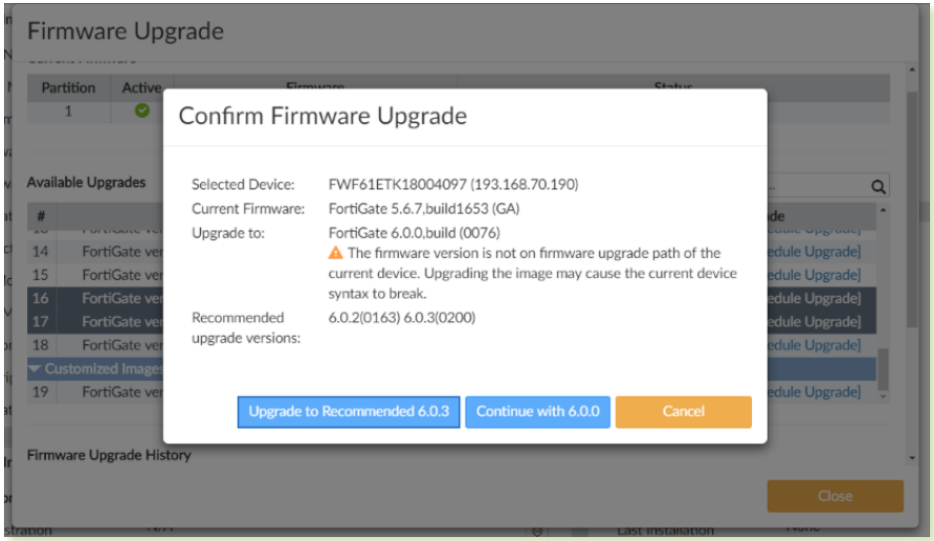
- Aktualisieren mehrerer FortiGate Devices mit dem empfohlenen Upgrade Pfad



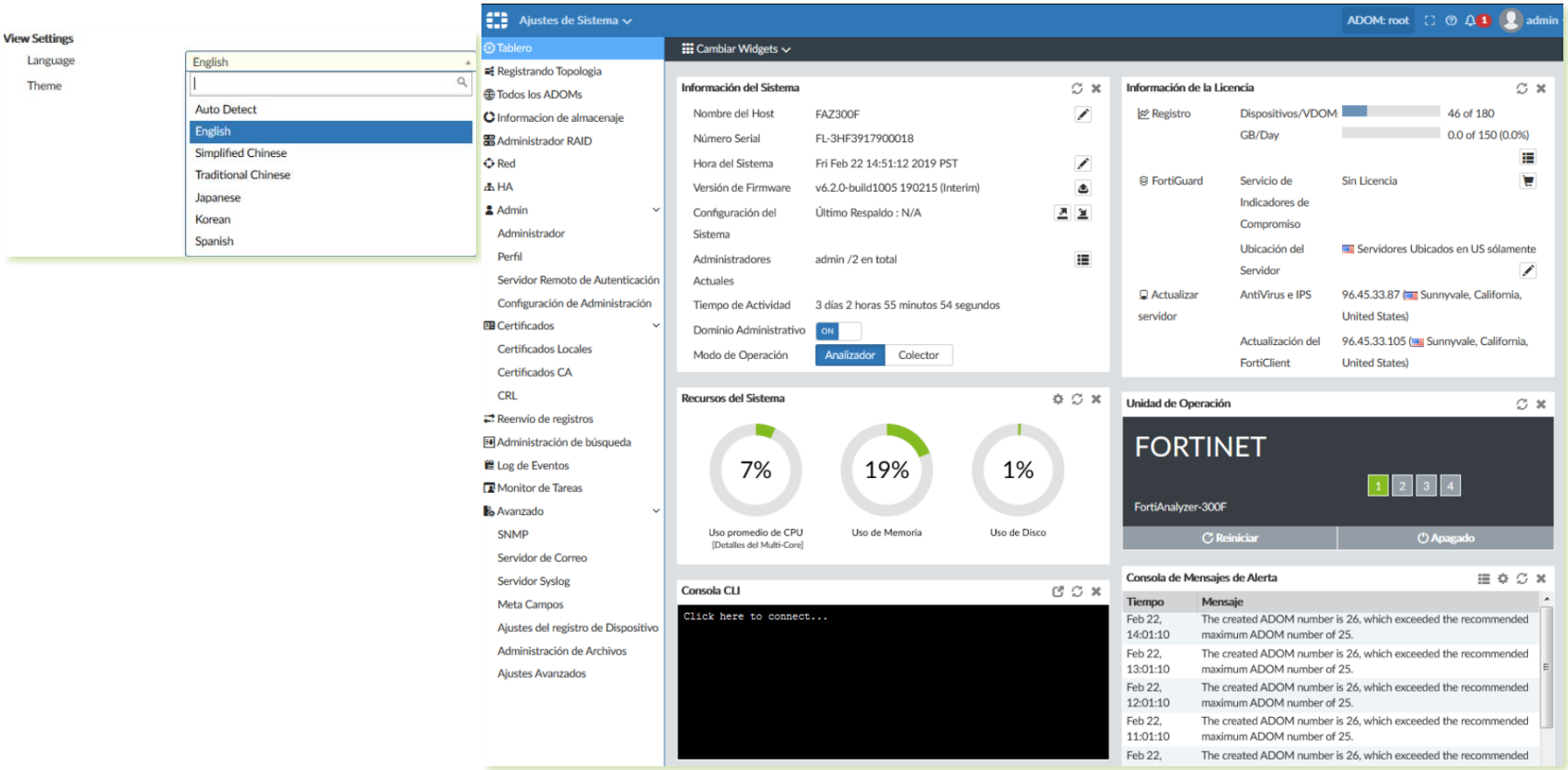


Individuelles Aktualisieren mit empfohlenem Upgrade Pfad

- Wenn eine Firmware ausgewählt wird die sich nicht auf dem upgrade Pfad befindet, wird eine Warnung mit der Option zum Aktualisieren mit dem empfohlenen Upgrade Pfad angezeigt.



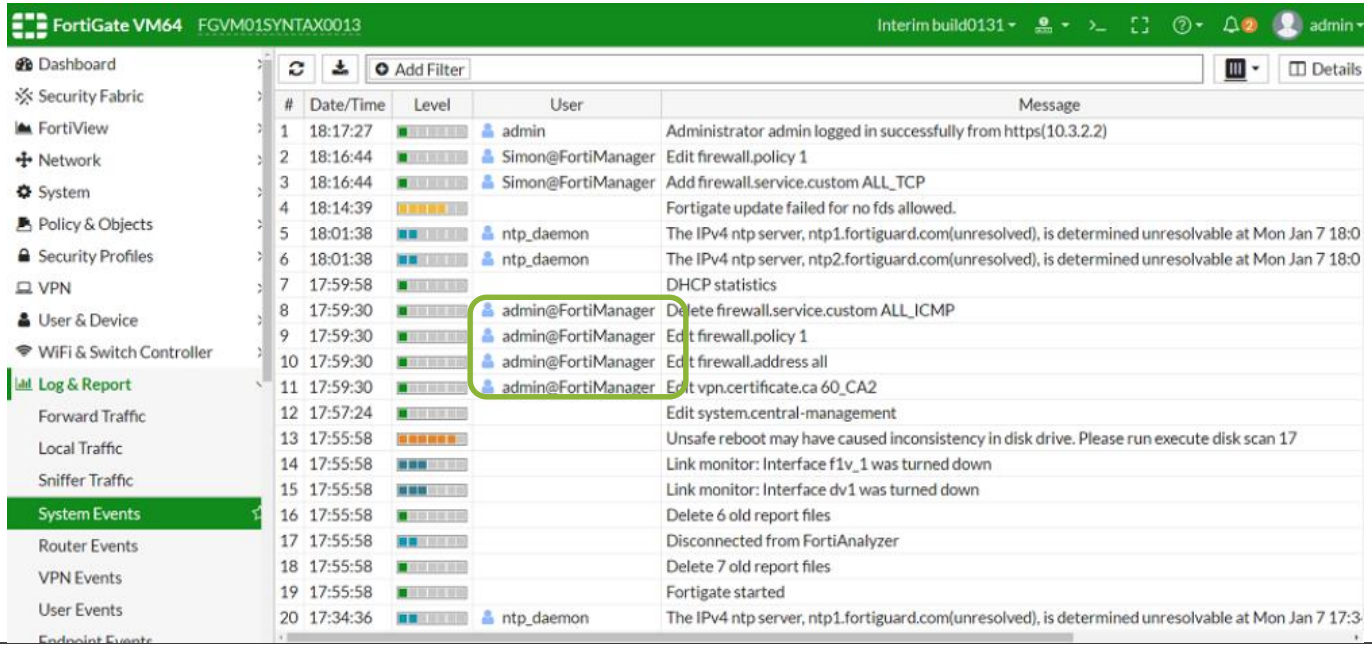
Spanische Oberfläche



Compliance

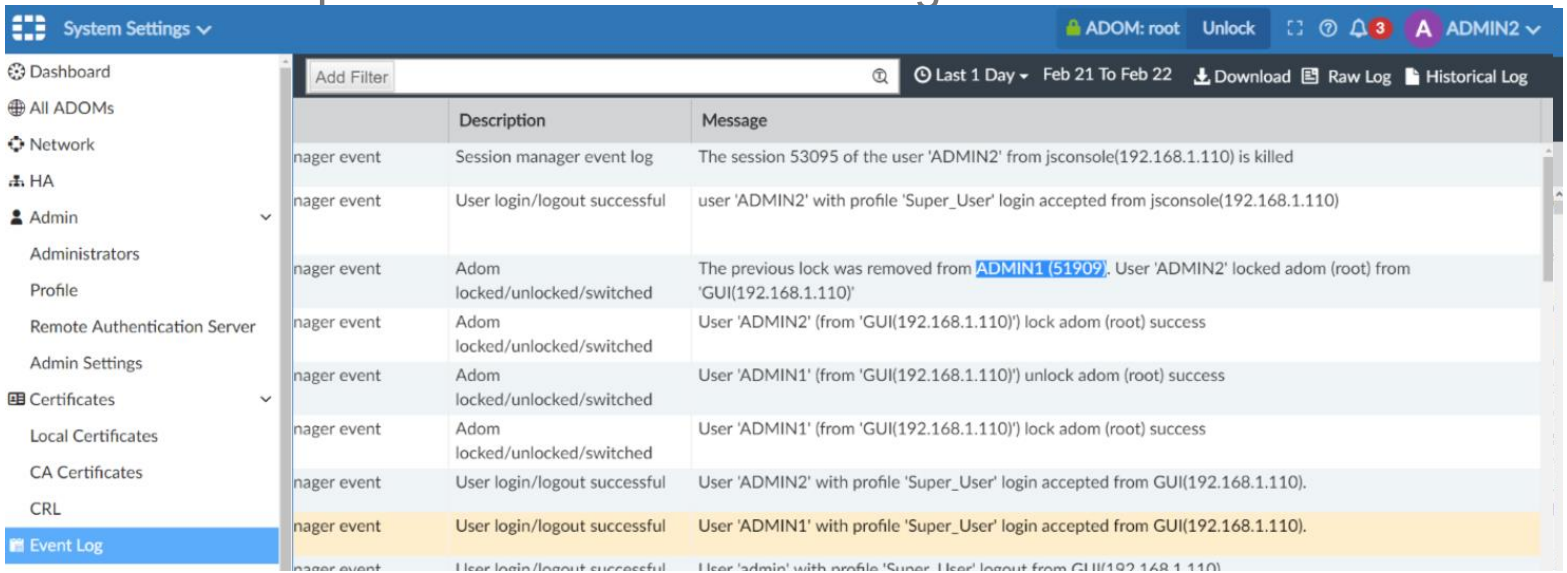
Änderung Change Log auf der FortiGate

- Wenn eine Änderung auf der FortiGate durch den FortiManager vorgenommen wird, ist diese jetzt klarer im Change Log ersichtlich



Modifikation Event Log

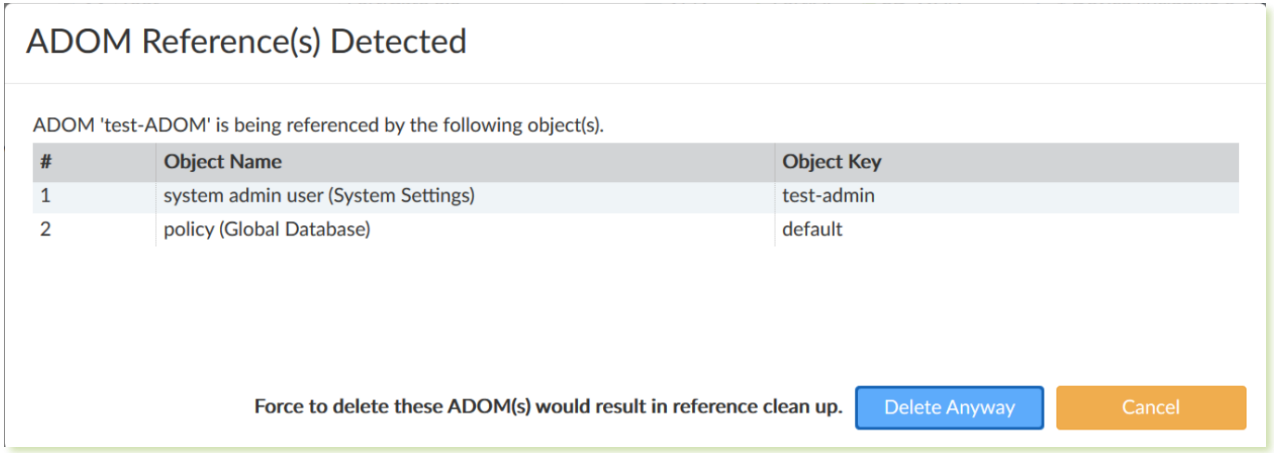
- Die Session ID wird zu jedem Logeintrag hinzugefügt
- Vorhandene Prüfsumme Linux Epochen-Zeitstempel, wird ein ein für Menschen Lesbares Format konvertiert
- ADOM Preempt Lock Takeover Event Logs sind klarer.



Other

Löschen von leeren ADOMs

- Alle Devices müssen in einer ADOM entfernt werden
- Die globalen Verknüpfungen werden neu gelöscht, wenn die ADOM gelöscht wird



Modifiziertes RADIUS Setting

- Testen der User Credentials
- Die Wildcard-Option wurde geändert, um alle Benutzer auf dem Remote-Server in der GUI abzugleichen.

```
config system admin user
    edit "Radius"
        set adom "all_adoms"
        set policy-package "all_policy_packages"
        set user_type radius
        set radius_server "test-Radius"
        set wildcard enable
        set ext-auth-accprofile-override enable
        set ext-auth-adom-override enable
    next
end
```